LISTING OF CLAIMS

1. **(Currently Amended)** A method of controlling access to a network, the method comprising:

configuring an authentication server to include a first location information corresponding to an identity of a mobile client, the first location information being a location at which the mobile client is permitted to connect to the network,

wherein the authentication server is coupled to the network and comprises a Remote Authentication Dial-In User Service (RADIUS) server having RADIUS attributes, and

wherein the first location information is included within a RADIUS vendor specific attribute (VSA) of the RADIUS attributes;

requesting by a network switch [[an]]the identity of the mobile client from [[a]]the mobile client attempting to connect to the network;

receiving, by the authentication server, the identity of the mobile client via the network switch;

associating, by the network switch, a second location information corresponding to the mobile client with the identity of the mobile client, wherein the second location information indicates a location of the network switch coupled to the network to which the mobile client is attempting to connect;

authenticating, by the authentication server, the identity of the mobile client received by the authentication server;

comparing, by the authentication server, the second location information corresponding to the mobile client against ~~a policy designating locations, if any,~~ the first location information from the VSA ~~at which the client is permitted to connect to the network~~; ~~and~~

deciding, by the authentication server, whether to grant or deny access to the network for the mobile client ~~access to the network based on~~ in response to ~~the authenticity of~~ authenticating the identity of the mobile client and in response to comparing the second location information against the first ~~comparison of the~~ location information; and

informing the network switch by the authentication server whether to grant or deny access to the network for the mobile client. ~~wherein the location information indicates the location of a network switch to which the client is attempting to connect, and the location information indicates the association between a particular port of the network switch and the physical location of an edge device or a wired user station associated with the particular port of the network switch.~~

2-3. **(Cancelled)**.

4. **(Currently Amended)** The method of claim 1, wherein the identity of the mobile client includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared encryption key, a smart card identifier, and any combination of the foregoing information.

5. **(Currently Amended)** The method of claim 1, wherein the mobile client is a user station capable of connecting to the network through an access point.

6. **(Currently Amended)** The method of claim 1, wherein the mobile client is a wired device capable of connecting to the network through an Ethernet switch port.

7. **(Currently Amended)** The method of claim 1, wherein authenticating the identity of the mobile client comprises ~~comprising:~~ authenticating the identity of the mobile client via ~~using~~ a mechanism selected from the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing ~~to authenticate the identity~~.

8. **(Cancelled)**.

9. **(Currently Amended)** The method of claim 1[[,]] further comprising:

storing the second location information on the network switch; and

periodically downloading the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the ~~location information indicates the location of an~~ edge device ~~for connecting the client to the network~~.

10. **(Currently Amended)** A network system[[,]] comprising:

a network;

an authentication server coupled to the network, the authentication server configured to include a first location information corresponding to an identity of a mobile client, the first location information being a location at which the mobile client is permitted to connect to the network,

wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server having RADIUS attributes, and

wherein the first location information is included within a RADIUS vendor specific attribute (VSA) of the RADIUS attributes;

a network switch coupled to the network and having an authenticator for requesting an identity from [[a]]the mobile client and for associating a second location information corresponding to the mobile client with the identity of the mobile client, wherein the mobile client is operable to communicate[[s]] to the authenticator of the network switch, and ~~from~~ ~~a~~ wherein the second location information indicates a location of the network switch coupled to the network to which the mobile client is attempting to connect;~~ user station;~~ and

~~a data structure, accessible by an authentication server, associating identities of clients with their authorized access locations;~~

~~the authentication server, upon receiving the identity and associated location information from the authenticator, deciding whether to grant or deny client access to the~~

~~network by accessing the data structure and determining that the location information corresponding to the client specifies a location that is one of the authorized access locations, if any, for the client as maintained in the data structure; and~~

a network manager comprising an application running on a server, wherein the application permits ~~the~~ a network administrator to create and update a policy table ~~in~~ of the authentication server, wherein the authentication server is operable to:

authenticate the identity of the mobile client received by the authentication server;

compare the second location information corresponding to the mobile client against the first location information from the VSA;

decide whether to grant or deny access to the network for the mobile client in response to authenticating the identity of the mobile client and in response to comparing the second location information against the first location information; and

inform the network switch whether to grant or deny access to the network for the mobile client.

11-12. (**Cancelled**).

13. (**Currently Amended**) The network system of claim 10, further comprising[[:]] an edge device for connecting a user station to [[a]]the network switch.

14. (Original) The network system of claim 13, wherein the edge device is a wireless access point.

15. (**Currently Amended**) The network system of claim 14, wherein the user station capable of connecting to the network through the wireless access point.

16. (**Currently Amended**) The network system of claim 10, wherein the mobile client is a wired device capable of connecting to [[a]]the network switch through an Ethernet port.

17-18. (**Cancelled**).

19. (**Currently Amended**) The network system of claim [[18,]]10 further comprising an interface for permitting an administrator to associate the second location information to the ~~edge device~~ mobile client.

20. (Original) The network system of claim 10, wherein the authentication server is included in a network switch.

21-23. (**Cancelled**).

24. (**Currently Amended**) The network system of claim 10, wherein the identity of the mobile client includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

25. (**Currently Amended**) The network system of claim 10, ~~further comprising a~~ wherein the network switch ~~that~~ comprises[[:]] an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

26. (**Currently Amended**) The network system of claim 10, wherein the authentication server comprises[[:]] an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

27-38 (**Cancelled**).

39. (**Currently Amended**) A network system for controlling access to a network, the network system comprising:

means for configuring an authentication server to include a first location information corresponding to an identity of a mobile client, the first location information being a location at which the mobile client is permitted to connect to the network,

wherein the authentication server is coupled to the network and comprises a Remote Authentication Dial-In User Service (RADIUS) server having RADIUS attributes, and

wherein the first location information is included within a RADIUS vendor specific attribute (VSA) of the RADIUS attributes;

means for requesting by a network switch [[an]]the identity of the mobile client from [[a]]the mobile client attempting to connect to the network;

means for receiving, by the authentication server, the identity of the mobile client via the network switch;

means for ~~first~~ associating ~~means for associating~~, by the network switch, a second location information corresponding to the mobile client with the identity of the mobile client, wherein the second location information indicates a location of the network switch coupled to the network to which the mobile client is attempting to connect;

means for authenticating ~~means for authenticating~~, by the authentication server, the identity of the mobile client received by the authentication server;

means for comparing, by the authentication server, the second location information corresponding to the mobile client against [[a]] ~~policy designating locations, if any,~~ the first location information ~~at which the client is permitted to connect to the network~~;

means for deciding, by the authentication server, whether to grant or deny access to the network for the mobile client ~~access to the network based on~~ in response to ~~the authenticity of~~ authenticating the identity of the mobile client and in response to comparing the second location information against the first ~~comparison of the~~ location information; and

means for informing the network switch by the authentication server whether to grant or deny access to the network for the mobile client.

~~a means for network management comprising a means for a server that runs an application that permits a network administrator the means to configure the location information and software images stored in means for switching; and~~

~~a network means that connects the means for network management, the means for authentication and the means for switching;~~

~~wherein the network system further comprises a means for network management, wherein the means for network management configures the means for authenticating,~~

~~wherein the means for network management either (1) connects to the network or (2) directly connects to the means for switching and directly connects to the means for authentication,~~

~~whereby when the means for network management directly connects to the means for switching and the means for authentication, the means for network is bypassed.~~

40. **(Currently Amended)** The network system of claim 39, wherein the identity of the mobile client includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

41. **(Currently Amended)** The network system of claim 39, wherein the mobile client is a wireless device capable of connecting to the network through an access point.

42. **(Currently Amended)** The network system of claim 39, wherein the mobile client is a wired device capable of connecting to the network through an Ethernet port.

43. **(Currently Amended)** The network system of claim 39, wherein the means for authentication includes:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

44-45. **(Cancelled)**.

46. **(Currently Amended)** The method of claim 1, wherein the mobile client is associated with a newly located access point upon authenticating the identity of the mobile client and determining, by comparing an updated location information corresponding to the mobile client against the first location information in the policy table, the first location information being the information that the mobile client is still authorized to access the network.

47. **(Cancelled)**.

48. **(Currently Amended)** The method of claim 8, wherein the second location information indicates ~~the~~ a location of a port of [[a]]the network switch to which the mobile client is attempting to connect.

49. **(Currently Amended)** The network system of claim [[17]]10, wherein the second location information indicates ~~the~~ a location of a port of [[a]]the network switch to which the mobile client is attempting to connect.

50. **(Currently Amended)** The network system of claim 24, wherein the identity of the mobile client includes a smart card identifier.

51. **(Cancelled)**.

52. (**New**) The network system of claim 10 further comprising:

means for storing the second location information on the network switch; and

means for periodically downloading the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the edge device.

53. (**New**) The network system of claim 39 further comprising:

means for storing the second location information on the network switch; and

means for periodically downloading the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the edge device.